UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/465,600	12/17/1999	ALEX I. EYDELBERG	INTL-0304-US	9073

21906 7590 04/21/2006

TROP PRUNER & HU, PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/465,600	EYDELBERG, ALEX I.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 1/30/06.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 31-37,39-41,43-51,53 and 55-63 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 31-37,39-41, 43-51, 53 and 55-63 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 31-37, 39-41, 43-51, 53, and 55-63 remains rejected and are pending.

2. This is a Non-Final rejection because claims 57-63 was not addressed in the previous office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. ***Claims 31-37, 39-41, 43-51, 53, and 55-63 are rejected under 35 U.S.C. 103(a) as being unpatentable by Rakavy, et. Al. (US 6,324,644) in view of Anderson (US 6,161,177) and Godse (US 6,202,091) and in further view of Kuznetsov, et al. (US 5,483,649).***

As per claim 31:

Rakavy teach having more than one BIOS with the ability to detect and load the network BIOS [see col.6, lines 35-60]. However, Rakavy did not go into details of loading either a first module of the basic input/output system or a second module of the basic input/output system based on a system state.

Anderson teaches a computer system that includes a memory device containing a BIOS program and BIOS identifying data specifying the CPU corresponding to the BIOS program. Further, Anderson teaches determining if the correct BIOS has been selected for execution by the CPU (col.4, lines 41-43 and col.5, lines 22-30). It would have been obvious of the ordinary skill in the art to combine the teachings of Rakavy with Anderson of being able to selectively load the first or second BIOS is to ensure that the proper BIOS program is executed in computer systems having more than one BIOS program retained in a storage device and this will add optimum performance (col.2, lines 45-63).

However, the Rakavy & Anderson combination did not include selectively load the bios based on the system state indicating a connection to the network.

Godse teaches avoiding the necessity of changing the boot-up program at each node of the network by including a pointer that can be selectively set to point toward a local site or a remote site that allows initiating the boot-up procedure locally while loading some software component such as a network wherein the component that are selected to load (col.2, lines 40-49 and col.4, lines 30-53). It would have been obvious of the ordinary skill in the art to combine the teachings of the Rakavy & Anderson

combination with Godse of being able to selectively load the BIOS based on the system state indicating a connection to a network because this avoids the necessity of changing the boot-up program at each node of the network (col.2, lines 49-50).

However, the combinations of Rakavy, Anderson, and Godse did not include requesting the first level of authentication information or a second level of authentication information from a user based on the system state.

Kuznetsov, et al. teaches a file protection subsystem is interfaced with the personal computer system to monitor the security of requests where the only permitted access path is using the BIOS (col.5, lines 53-60) and there includes a program that checks requests at the BIOS level (col.6, lines 20-22). Kuznetsov discloses access control profile that includes the identity of the user and the authorization level granted to each listed user (col.3, lines 10-15). Kuznetsov disclose the protection initialization program that identifies the personal computer user and the BIOS-level request check program checks for a match between the current request and the set of dangerous request at the BIOS level thereby prevents the servicing of dangerous requests (col.7, lines 40-48 and col.9, lines 32-35). Hence, by requesting a safe authentication level, the PRM switches to a passive operating mode and based on the system state where an attempt to use the hard disk controller when the PRM is in the active mode will result in the removal of the CPU availability (col.7, lines 50-58). Further, the (13h) BIOS program interrupt loads the protection kernel into the main memory where after the protection kernel is loaded, the protection initialization program will request user password (col.9, lines 55-58). Kuznetsov discloses based on the system state

indicative of a connection is when the protection kernel is loaded or not. The authentication information from the user is the password when requested if after the system state has loaded the protection kernel. Thus, based on the system state indicative of a connection is where the CPU stops if the authentication information from the user such as the password does not match (col.9, lines 60-67). It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of the Rakavy & Anderson & Godse combination with Kuznetsov of requesting the first level of second level of authentication information from a user based on the system state indicative of a connection because based on the protection kernel has to be loaded for the system state to request a user password for a connection and the BIOS-level request check program prevents servicing of dangerous requests.

As per claim 32:

Rakavy, et al. discloses a method of claim 1 further comprising:

storing said first module of a basic input/output system on a first storage device prior to execution; **[see col.6, lines 45-56]**

storing said second module of the basic input/output system on a second storage device prior to execution; and **[see col.5, lines 47-51]**

enabling said second module to be executed conditionally depending on a state. **[see col.7, lines 13-26 and col.8, lines 7-29]**

As per claim 33: see Rakavy on FIGs.1 and 7; discussing storing said second module includes storing said second module in a storage associated with a network server accessible to said system over the network.

As per claim 34: **see Rakavy on col.9, lines 23- 43;** discussing detecting whether or not the system is connected to the network during a boot sequence.

As per claim 35: **see Rakavy on col.7, lines 25-33 and col.8, lines 1-6;** discusses dynamically linking to one of a plurality of modules, and exporting and offset to an entry point in one module to another module.

As per claim 36: **see Rakavy on col. 8, lines 7-29;** discusses storing a secondary entry point in a module to locate a function within the module.

As per claim 37: **see Rakavy on col.15, lines 26-43 and FIG.3A;** discusses developing a segment address for said second module at run time.

As per claim 38: **Cancelled.**

As per claim 39: **see Rakavy on col.5, lines 40-55 and col.9, lines 43-56;** discusses authenticating a user according to one of multiple levels based upon the system state, and obtaining a key from a protected storage if the user is authenticated.

As per claim 40:

Rakavy teach having more than one BIOS with the ability to detect and load the network BIOS [see col.6, lines 35-60]. However, Rakavy did not go into details of loading either a first module of the basic input/output system or a second module of the basic input/output system based on a system state.

Anderson teaches a computer system that includes a memory device containing a BIOS program and BIOS identifying data specifying the CPU corresponding to the BIOS program. Further, Anderson teaches determining if the correct BIOS has been selected for execution by the CPU (col.4, lines 41-43 and col.5, lines 22-30). It would

have been obvious of the ordinary skill in the art to combine the teachings of Rakavy with Anderson of being able to selectively load the first or second BIOS is to ensure that the proper BIOS program is executed in computer systems having more than one BIOS program retained in a storage device and this will add optimum performance (col.2, lines 45-63).

However, the Rakavy & Anderson combination did not include selectively load the bios based on the system state indicating a connection to the network.

Godse teach a pointer that can be selectively set to point toward a local site or a remote site that allows initiating the boot-up procedure locally while loading some software component such as a network wherein the component that are selected to load (col.2, lines 40-49 and col.4, lines 30-53). It would have been obvious of the ordinary skill in the art to combine the teachings of the Rakavy & Anderson combination with Godse of being able to selectively load the BIOS based on the system state indicating a connection to a network because this avoids the necessity of changing the boot-up program at each node of the network (col.2, lines 49-50).

Kuznetsov, et al. teaches a file protection subsystem is interfaced with the personal computer system to monitor the security of requests where the only permitted access path is using the BIOS (col.5, lines 53-60) and there includes a program that checks requests at the BIOS level (col.6, lines 20-22). Kuznetsov discloses access control profile that includes the identity of the user and the authorization level granted to each listed user (col.3, lines 10-15). Kuznetsov disclose the protection initialization program that identifies the personal computer user and the BIOS-level request check

program checks for a match between the current request and the set of dangerous request at the BIOS level thereby prevents the servicing of dangerous requests (col.7, lines 40-48 and col.9, lines 32-35). Hence, by requesting a safe authentication level, the PRM switches to a passive operating mode and based on the system state where an attempt to use the hard disk controller when the PRM is in the active mode will result in the removal of the CPU availability (col.7, lines 50-58). Further, the (13h) BIOS program interrupt loads the protection kernel into the main memory where after the protection kernel is loaded, the protection initialization program will request user password (col.9, lines 55-58). Kuznetsov discloses based on the system state indicative of a connection is when the protection kernel is loaded or not. The authentication information from the user is the password when requested if after the system state has loaded the protection kernel. Thus, based on the system state indicative of a connection is where the CPU stops if the authentication information from the user such as the password does not match (col.9, lines 60-67). It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of the Rakavy & Anderson & Godse combination with Kuznetsov of requesting the first level of second level of authentication information from a user based on the system state indicative of a connection because based on the protection kernel has to be loaded for the system state to request a user password for a connection and the BIOS-level request check program prevents servicing of dangerous requests.

As per claim 41:

Rakavy, et al. discloses a method of claim 1 further comprising:

access said first module of a basic input/output system on a first storage device; **[see col.6, lines 45-56]**

access said second module of the basic input/output system on a second storage device; and **[see col.5, lines 47-51]**

execute said second module conditionally depending on a state. **[see col.7, lines 13-26 and col.8, lines 7-29]**

As per claim 42: Cancelled.

As per claim 43: see Rakavy on col.7, lines 13-26 and col.8, lines 7-29; discusses storing instructions that cause a system to execute said second module conditionally depending on whether or not the system is coupled to the network.

As per claim 44: see Rakavy on col.13, line 40 thru col.14, line 49; discusses storing instructions that cause a system to selectively access either a first module setting forth a first authentication protocol in the first storage device or a second module setting forth a second authentication protocol in the second storage device based on the system state.

As per claim 45: see col.5, lines 40-55 and col.9, lines 43-56; discusses storing instructions that cause a system to obtain a key from a protected storage if a user is authenticated.

As per claim 46: see Rakavy on col.7, lines 25-33 and col.8, lines 1-6; discusses storing instructions that cause a system to dynamically link said first and second modules.

As per claim 47: **see Rakavy on col.9, lines 23- 43;** discusses storing instructions that cause a system to detect whether the system is connected to the network during a boot sequence.

As per claim 48: **see Rakavy on col.7, lines 25-33 and col.8, lines 1-6;** discusses storing instructions that cause a system to dynamically link to one of a plurality of modules using offsets to entry points in said modules.

As per claim 49: **see Rakavy on col.7, lines 25-33 and col.8, lines 1-6;** discusses storing instructions that cause a system to store a secondary entry point in a module to locate a function within the module.

As per claim 50: **See Rakavy on col.15, lines 26-43 and FIG.3A;** discusses storing instructions that cause a system to develop a segment address for said second module at run time.

As per claim 51:

Rakavy discloses system comprising:

a first basic input/output system module executable by a processor; and **[see col.5, lines 46-48 and col.6, lines 24-63]**

a second basic input/output system module executable by said processor; and **[see col.12, line 56 thru col.13, line 2 and col.15, lines 3-13]**

However, Rakavy fails to discuss loading either a first module of the basic input/output system or a second module of the basic input/output system based on a system state.

Anderson teaches a computer system that includes a BIOS program and BIOS identifying data specifying the CPU corresponding to the BIOS program and determining if the correct BIOS has been selected for execution by the CPU (col.4, lines 41-43 and col.5, lines 22-30). The EEPROM stores the system BIOS program which is the first BIOS module stored in the first storage of the system that is executed by the CPU (col.4, lines 20 and 47-54). Anderson discusses the startup program is stored in a memory device different from the EEPROM (col.4, lines 37-39) and another storage is the disk drive of the system that contains the correct BIOS program (col.5, lines 5-17). It would have been obvious of the ordinary skill in the art to combine the teachings of Rakavy with Anderson of being able to selectively load the first or second BIOS of a first and second storage (col.2, lines 45-63) is to ensure that the proper BIOS program is executed in computer systems having more than one BIOS program retained in a storage device adding optimum performance and crisis recovery purposes.

However, the Rakavy & Anderson combination fails to include selectively load the bios based on the system state indicating a connection to the network.

Godse teach a pointer that can be selectively set to point toward a local site or a remote site that allows initiating the boot-up procedure locally while loading some software component such as a network wherein the component that are selected to load (col.2, lines 40-49 and col.4, lines 30-53). It would have been obvious of the ordinary skill in the art to combine the teachings of the Rakavy & Anderson combination with Godse of being able to selectively load the BIOS based on the system state indicating a

connection to a network because this avoids the necessity of changing the boot-up program at each node of the network (col.2, lines 49-50).

Kuznetsov, et al. teaches a file protection subsystem is interfaced with the personal computer system to monitor the security of requests where the only permitted access path is using the BIOS (col.5, lines 53-60) and there includes a program that checks requests at the BIOS level (col.6, lines 20-22). Kuznetsov discloses access control profile that includes the identity of the user and the authorization level granted to each listed user (col.3, lines 10-15). Kuznetsov disclose the protection initialization program that identifies the personal computer user and the BIOS-level request check program checks for a match between the current request and the set of dangerous request at the BIOS level thereby prevents the servicing of dangerous requests (col.7, lines 40-48 and col.9, lines 32-35). Hence, by requesting a safe authentication level, the PRM switches to a passive operating mode and based on the system state where an attempt to use the hard disk controller when the PRM is in the active mode will result in the removal of the CPU availability (col.7, lines 50-58). Further, the (13h) BIOS program interrupt loads the protection kernel into the main memory where after the protection kernel is loaded, the protection initialization program will request user password (col.9, lines 55-58). Kuznetsov discloses based on the system state indicative of a connection is when the protection kernel is loaded or not. The authentication information from the user is the password when requested if after the system state has loaded the protection kernel. Thus, based on the system state indicative of a connection is where the CPU stops if the authentication information from

the user such as the password does not match (col.9, lines 60-67). It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of the Rakavy & Anderson & Godse combination with Kuznetsov of requesting the first level of second level of authentication information from a user based on the system state indicative of a connection because based on the protection kernel has to be loaded for the system state to request a user password for a connection and the BIOS-level request check program prevents servicing of dangerous requests.

As per claim 52: Cancelled.

As per claim 53: see Rakavy on col.5, lines 47-65 and col.7, lines 23-31 and Anderson on col.5, lines 22-30; discusses a third basic input/output module stored in a third storage, said third storage being coupled to said system over the network.

As per claim 54: Cancelled.

As per claim 55: see Rakavy on col.9, lines 43-62 and col.13, lines 26-63; discusses first and second basic input/output module modules include different authentication protocols.

As per claim 56: see Rakavy on col.13, line 40 thru col.14, line 49; discusses processor to execute said second basic input/output system module to implement a network authentication protocol.

As per claim 57: see Kuznetsov on col.3, lines 10-18 and col.9, lines 55-67; the first level of authentication information is greater than the second level of authentication information and further comprising requesting the first level of authentication information if the system is connected to the network.

As per claim 58: see Rakavy on col.5, lines 42-44 and Anderson on col.4, lines 37-39; a fourth basic input/output system module stored in a fourth storage.

As per claim 59: see Rakavy on col.5, lines 42-44 disclosing different types of computers such the ATM or point of sale terminals is a card reader that reads a card; a card reader coupled to the processor, the card reader to read a card, wherein the card comprises the fourth storage.

As per claim 60: see Rakavy on col.5, lines 42-44; the fourth storage comprises a smart card.

As per claim 61: see Kuznetsov on col.3, lines 10-18 and col.9, lines 55-67; executing the loaded one of the first basic input/output system module or the second basic input/output system module to request the authentication information from the user and authenticate the user.

As per claim 62: see Rakavy on col.5, lines 42-44 disclosing different types of computers such the ATM or point of sale terminals is a card reader that reads a card; the first level of authentication information includes presence of a smart card in the system.

As per claim 63: see Rakavy on col.9, lines 50-56; authenticating the user a second time after an operating system is loaded.

Response to Arguments

Claims 57-63 have been addressed and rejected. The rejection for claims 31-37, 39-41, 43-51, and 53 remains rejected. This office action is non-final because claims 57-63 was not addressed in the previous rejection.

As per claim 51, Anderson discloses the EEPROM stores the system BIOS program which is the first BIOS module stored in the first storage of the system that is executed by the CPU (col.4, lines 20 and 47-54). Anderson discusses the startup program is stored in a memory device different from the EEPROM (col.4, lines 37-39) and another storage is the disk drive of the system that contains the correct BIOS program (col.5, lines 5-17). Therefore, Anderson does disclose the first and second BIOS modules stored in different storages of a system.

As per claims 31 and 40, Kuznetsov discloses the known access control profile that includes an authorization parameter listing the identities of users and the authorization level granted to each listed user (col.3, lines 10-15) and teaches an improvement to this known technique by providing the operator with a personal having hidden storage of security programs and prevent unauthorized access (col.4, lines 16-23). Kuznetsov discusses that after the protection kernel is loaded, the protection initialization program will request user password (col.9, lines 55-58). Kuznetsov discloses based on the system state indicative of a connection is when the protection kernel is loaded or not. The authentication information from the user is the password when requested if after the system state has loaded the protection kernel. Thus, based on the system state indicative of a connection is where the CPU stops if the

authentication information from the user such as the password does not match (col.9, lines 60-67).

The commonalities of the Rakavy, Anderson, Godse, and Kuznetsov inventions is the teachings of the BIOS and preventing unauthorized access. Rakavy's invention teaches having more than one BIOS with the ability to detect and load the network BIOS [see col.6, lines 35-60]. Anderson's invention teaches determining if the correct BIOS has been selected for execution by the CPU (col.4, lines 41-43 and col.5, lines 22-30). Anderson teaches the EEPROM storing the system BIOS program which is the first BIOS module stored in the first storage of the system that is executed by the CPU (col.4, lines 20 and 47-54) and the startup program is stored in a memory device different from the EEPROM (col.4, lines 37-39) and another storage is the disk drive of the system that contains the correct BIOS program (col.5, lines 5-17). It would have been obvious of the ordinary skill in the art to combine the teachings of Rakavy with Anderson of being able to selectively load the first or second BIOS is to ensure that the proper BIOS program is executed in computer systems having more than one BIOS program retained in a storage device and this will add optimum performance (col.2, lines 45-63). Godse's invention teaches a pointer that can be selectively set to point toward a local site or a remote site that allows initiating the boot-up procedure locally while loading some software component such as a network wherein the component that are selected to load (col.2, lines 40-49 and col.4, lines 30-53) where it would have been obvious of the ordinary

skill in the art to combine the teachings of the Rakavy & Anderson combination with Godse of being able to selectively load the BIOS based on the system state indicating a connection to a network because this avoids the necessity of changing the boot-up program at each node of the network (col.2, lines 49-50). Finally, Kuznetsov's invention teaches different levels of authentication information of a user in the form of access control profile that includes the identity of the user and the authorization level granted to each listed user (col.3, lines 10-15) and further discusses that after the protection kernel is loaded, the protection initialization program will request user password (col.9, lines 55-58). Kuznetsov discloses based on the system state indicative of a connection is when the protection kernel is loaded or not. The authentication information from the user is the password when requested if after the system state has loaded the protection kernel. Thus, based on the system state indicative of a connection is where the CPU stops if the authentication information from the user such as the password does not match (col.9, lines 60-67). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of the Rakavy & Anderson & Godse combination with Kuznetsov of requesting the first level of second level of authentication information from a user based on the system state indicative of a connection because based on the protection kernel has to be loaded for the system state to request a user password for a connection and

the BIOS-level request check program prevents servicing of dangerous requests.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100